TRAI	TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c)) Docket No. 00001-0423								
In Re Application Of: Robert J. Lambert et al.									
Serial No. Filing Date Examiner Group Art Unit									
	10/058,214 January 29, 2002 Not Yet Assigned 2131								
Title: METHOD AND APPARATUS FOR ELLIPTIC CURVE SCALAR MULTIPLICATION OF E COLUMN 10 8 2000 25 PECEIVED									
SATENT & T	MEET	. "	ddress to:	1.07 1.0.2002					
W/8 T	RADER		missioner for Patents on, D.C. 20231	MAY 1 0 2002					
				nnology Center 2100					
		37 CI	FR 1.97(b)						
1. 🔀	of a national app CFR 1.491 in a	Disclosure Statement submitted plication; within three months of the international application; or been event occurs last. 37 CI	he date of entry of the nationa	I stage as set forth in 37					
2. 🗆	of a national appointernational app	Disclosure Statement submitted plication, or the date of entry of plication; or after the mailing date of either	the national stage as set forthate of a first Office Action of	n in 37 CFR 1.491 in an					
	1.	a Final Action under 37 CFR 1.1	13, or						
	2.	a Notice of Allowance under 37 C	OFR 1.311,						
	whichev	er occurs first.							
	Also submitted h	nerewith is:	·						
	☐ a certifica	tion as specified in 37 CFR 1.97(e);						
OR									
		et forth in 37 CFR 1.17(p) for s CFR 1.97(c).	cubmission of an Information	Disclosure Statement					

Copyright 1996 Legalsoft P10A/REV01

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c)) Docket No. 00001-0423								
In Re Application Of: Robert J. Lambert et al.								
Serial No. Filing Date Examiner Gro								
10/058,214 January 29, 2002 Not Yet Assigned 213								
RECEIVED								
Pres CHIEF			MAY 1 0 2002					
TRADEMAN	Paym	ent of Fee	47(n))					
	Paym (Only complete if Applicant elects t	to pay the fee set forth in 37 of it	echhology Center 2100					
A check in the am			 					
	mmissioner is hereby authorized	- · · · · · · · · · · · · · · · · · · ·	Account No. 150633					
	w. A duplicate copy of this shee	t is enclosed.						
	ne amount of							
·	y overpayment. ny additional fee required.							
⊠ Charge a	ny additional lee required.							
Certificate of	Transmission by Facsimile*	Certificate of Mailin	g by First Class Mail					
I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No.								
	Signature	Signature of Person M	failing Correspondence					
Typed or Printed !	Name of Person Signing Certificate	Typed or Printed Name of Pe	erson Mailing Correspondence					
*This certificate may only be used if paying by deposit account. Dated: May 3, 2002 Signature John R. S. Orange Orange & Chari 66 Wellington Street West Toronto Dominion Bank Tower Toronto, Ontario M5K 1H6								
cc:								

ATTORNEY DOCKET NO.:

00001-0423

STOMER NUMBER:

27,155

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

patent application of:

RECEIVED

MAY 1 0 2002

Serial No.:

10/058,214

Group Art Unit:

²¹³¹ Technology Center 2100

Filed:

01/29/2002

Examiner:

Not Yet Assigned

Title:

METHOD AND APPARATUS FOR ELLIPTIC CURVE SCALAR

MULTIPLICATION

LAMBERT, Robert J. et al.

Commissioner of Patents and Trademarks Washington, D.C. 20231

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08A listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each document listed in the enclosed Form PTO/SB/08A is submitted herewith.

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08A after being marked as being considered by the Examiner.

Respectfully submitted,

John R.S. Orange Registration No. 29,725 Agent/Attorney for Applicant

Orange & Chari Suite 4900, P.O. Box 190 66 Wellington Street West Toronto, Ontario M5K 1H6, Canada

Tel: (416) 601-8440 Fax: (416) 601-8454

PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO **Application Number** INFORMATION DISCLOSURE Filing Date STATEMENT BY APPLICANT **First Named Inventor**

(use as many sheets as necessary)

of

Complete if Known 10/058,214 01-29-2002 LAMBERT, Robert J. Art Unit **Examiner Name** Not Yet Assigned **Attorney Docket Number** 00001-0423

Sheet

إل	U.S. PATENT DOCUMENTS						
Examiner Initials		Cite No. ¹			Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
Ī			US- 6,212,279		04-03-2001	Robert W. Reiter, Jerome Solinas	
			US- 6,243,46°	7 B1	06-05-2001	Robert W. Reiter, Jerome Solinas	
	US-						
			US-				
			US-				
			US-				
Γ			US-				
			US-				
L			US-				
L			US-			DEC	FIVED
L			US-			NEU NEU	EIVED
			US-		<u></u>		4 0 000
L			US-			MAY	1 0 2002
			US-				
Γ			US-			Lechnolo	gy Center 2100
US- US-			US-			A A Description .	<u> </u>
			US-		-		
			US-				
ſ			US-				

	FOREIGN PATENT DOCUMENTS								
Cuamina.	0:1-	Foreign Patent Document			Publication Date	Name of Patentee or	Pages, Columns, Lines, Where Relevant		
Examiner Initials*	Cite No. ¹	Office ³	Number ⁴	Kind⁵ (if known)	MM-DD-YYYY	Applicant of Cited Document	Passages or Relevant Figures Appear		
							ĺ		
			- <u>-</u>						
			<u> </u>						

	 <u> </u>		
Examiner		Date	
Signature		Considered	_

¹ Applicant's unique citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 3 Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language Translation is attached.



^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Complete if Known **Application Number** 10/058.214 Filing Date 01-29-2002 **First Named Inventor** LAMBERT, Robert J. Group Art Unit **Examiner Name** Not Yet Assigned Attorney Docket Number 00001-0423

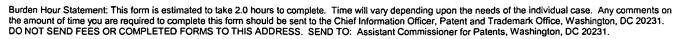
(use as many sheets as necessary)

heet

OTHER PRIOR ART NON PATENT LITERATURE DOCUMENTS						
Examiner Initials* Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.						
		JEROME A. SOLINAS, An Improved Algorithm for Arithmetic on a Family of Elliptic Curves, Advances in Cryptology - CRYPTO '97, 1997, 357-371.				
		JEROME A. SOLINAS, Improved Algorithms for Arithmetic on Anormalous Binary Curves, Technical Report, 1999. Available at http://cacr.uwaterloo.ca.				
			$\frac{1}{1}$			
		RECEIVED				
		MAY 1 0 2002				
		RECEIVED MAY 1 0 2002 Technology Center 2100				
		·				
-			_			

Examiner		Date	
Signature	·	Considered	

¹ Applicant's unique citation designation number (optional). ²Applicant is to place a check mark here if English language Translation is attached.



^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.